ABSTRACT

Described are techniques used for assessing the security of a network. Pruned attack trees are generated using a forward chaining, breadth-first technique representing the attack paths of a possible attacker in the network. A vulnerability score is determined for each network and attacker starting point using attack loss values assigned to each host and information extracted from the attack tree(s) concerning compromised hosts. Different hypothetical alternatives may be evaluated to improve security of the network and each alternative may be evaluated by recomputing the network vulnerability score and comparing the recomputed score to the original network vulnerability score. Also disclosed is a method for determining end-to-end connectivity of a network. The resulting end-to-end connectivity information is used in generating the pruned attack tree.